Kohärenzsicherung im unionalen Datenschutzrecht und ihre Grenzen

Gastautor 2019-06-17T23:17:18

von
MATTHIAS ZUSSNER

Daten haben für wirtschaftlichen Wettbewerb von jeher einen besonderen Stellenwert gehabt. In Verknüpfung mit dem passenden Kontext verschaffen Daten den Teilnehmern des allgemeinen Wirtschaftsverkehrs erst jene Informationen, die in der Folge über wirtschaftlichen Erfolg entscheiden. Hinzu kommt im digitalen Zeitalter, dass im Windschatten technischer Innovationen auch wirtschaftliche Geschäftsmodelle selbst einem umfassenden Digitalisierungsprozess unterliegen. Herkömmliche körperliche Wirtschaftsgüter erhalten immer weitreichendere und bisweilen auch sehr persönliche Datenbezüge und werden schon jetzt von einem breiten Angebot digitaler Dienstleistungen flankiert.

Der freie Verkehr von Daten wird damit zur notwendigen Grundlage eines gemeinsamen europäischen Datenraums und bleibt damit zentraler Baustein eines funktionsfähigen digitalen Binnenmarkts. Doch hat die Politik längst begriffen, dass die Abschaffung jedweder Blockaden des freien Datenverkehrs paradoxerweise die Selbstauflösung der europäischen Digitalwirtschaft bedeuten würde. Verbraucher müssen erst das notwendige Vertrauen in die Sicherheit von Datenverarbeitungen haben, damit sie personenbezogene Daten preisgeben und die Vorteile der Digitalisierung konsumieren wollen. Gewisse Blockaden des freien Datenverkehrs, nämlich aus Gründen der Privatsphäre und des Datenschutzes, bilden so gesehen eine entscheidende Voraussetzung dafür, dass Daten im Rahmen des Wirtschaftsverkehrs überhaupt fließen werden; umso eher freilich, wenn Daten

Grenzen überschreiten sollen und sich deren Folgeverarbeitungen in der Folge für gewöhnlich ungleich schwerer kontrollieren lassen.

Kohärenz im Datenschutzrecht

Zumal datenbezogenes Recht für den wirtschaftlichen Wettbewerb hochrelevant ist, besteht eine entscheidende Schwierigkeit darin, nicht nur ein jeweiliges Mindestniveau an Datenschutz in den einzelnen Mitgliedstaaten zu gewährleisten, sondern zur Erreichung gleicher Wettbewerbsbedingungen überhaupt eine einheitliche Anwendung des Datenschutzrechts innerhalb der gesamten Europäischen Union (EU) sicherzustellen. Als neuer allgemeiner EU-Rechtsrahmen für den Schutz personenbezogener Daten enthält die Datenschutz-Grundverordnung (DSGVO) zu diesem Zweck in Kapitel VII neue Regeln über die Zusammenarbeit der nationalen Datenschutzaufsichtsbehörden als Instrument der Sicherung ihrer kohärenten Anwendung. Neben der Ermöglichung gemeinsamer Maßnahmen von Aufsichtsbehörden verschiedener Mitgliedstaaten auf eigenem oder fremden Territorium wird nicht nur die Rechtsgrundlage zur wechselseitigen Amtshilfeverpflichtung reformuliert, sondern auch ein besonders intensives Abstimmungsverfahren „betroffener“ Aufsichtsbehörden im Fall von grenzüberschreitenden Datenverarbeitungen eingeführt. Flankierend wird mit dem sogenannten Kohärenzverfahren auch ein Konfliktlösungsmechanismus für auftretende Streitfälle im Netzwerk der europäischen Datenschutzaufsicht zur Seite gestellt, die durch verbindlichen Beschluss des Europäischen Datenschutzausschuss (ESDA) entschieden werden können.

Konstruktion(-sfehler) der Datenschutzaufsicht

Wie die Zusammenarbeit im Netzwerk der nationalen und europäischen Aufsichtsbehörden nach Maßgabe der DSGVO genau funktioniert, lässt sich indes erst durch Gesamtzusammenschau verschiedenster Einzelbestimmungen der DS-GVO erschließen. Diese sind aber nicht nur von einer Vielzahl an Quer- und Wechselverweisen geprägt und daher schwer „zugänglich“. Sie weisen vielmehr schon ganz grundsätzliche Konstruktionsfehler auf. Wenn die EU-Kommission in einer Mitteilung meint, dass „der neu geschaffene Mechanismus der federführenden Aufsichtsbehörde […] sicher[stellt], dass in der EU für die Aufsicht über ein Unternehmen, das Daten grenzüberschreitend verarbeitet, nur noch eine Datenschutzbehörde zuständig ist“ (COM[2017] 9 final, 2), muss dem schon dem Grunde nach zweierlei entgegengehalten werden: Erstens geht die DS-GVO von einem ganz bestimmten Begriff der Grenzüberschreitung aus, die nicht jeden Fall tatsächlicher Grenzüberschreitung erfasst und das one-stop-shop-Prinzip schon insofern stark „durchlöchert“. Zweitens sieht die DS-GVO zum Teil selbst dann Ausnahmen vom one-stop-shop-Prinzip vor, wenn eine Grenzüberschreitung in ihrem selbst festgelegten Sinn vorliegt. Wo das one-stop-shop-Prinzip nicht zur Anwendung kommt bleibt es daher bei der als überwunden geglaubten Zuständigkeitszersplitterung zwischen den nationalen Aufsichtsbehörden mit entsprechenden Folgefragen in Bezug auf Reichweite und Grenzen der Befugnisse nationaler Aufsichtsbehörden im Zusammenhang mit – jedenfalls tatsächlich – grenzüberschreitenden Datenverarbeitungen.

Die übrigen Regelungen der Zusammenarbeit nationaler Aufsichtsbehörden innerhalb und außerhalb des Kohärenzverfahrens greifen zum Teil stark ineinander, sind aber auch nicht durchwegs miteinander verknüpft bzw einander nachgeschaltet. Der ESDA ist in der Folge nicht zwingend, sondern eher punktuell nach Anrufung in den Prozess der Sicherstellung einer einheitlichen Rechtsanwendung involviert, womit sich das System der Zusammenarbeit der Aufsichtsbehörden nach Maßgabe der DSGVO insgesamt als ein eher ernüchternder Versuch der gegenstandsnotwendigen Sicherung gleichmäßiger Rechtsanwendung durch alternative Steuerungsmodi qualifizieren lässt. Von weiteren Detailproblemen ganz zu schweigen.

Zitiervorschlag: Matthias Zußner, Kohärenzsicherung im unionalen Datenschutzrecht und ihre Grenzen, JuWissBlog Nr. 67/2019 v. 19.6.2019, https://www.juwiss.de/67-2019/